AMENDMENTS TO THE SPECIFICATION

Please delete the paragraph beginning at page 5, line 11, and ending at page 5, line 16, and insert in its place the following replacement paragraph, which is marked to show all changes relative to the original paragraph:

The verifier V now chooses one of two questions to ask prover P. The prover does not know in advance which of these two questions he is going to be asked, but he will only be able to answer both of them correctly if he genuinely knows the secret s. The verifier V ~~prover~~ can ask either for the value of the product $r.s$ mod n, or for the value of r that the prover has just chosen.

Please delete the paragraph beginning at page 11, line 20, and ending at page 11, line 27, and insert in its place the following replacement paragraph, which is marked to show all changes relative to the original paragraph:

With reference to figure 3, in the modified protocol according to the present invention, all the numbers are given in Montgomery representation and all computations are done using Montgomery arithmetic. The secret of the prover P is set $\in Z_n$ (step 310) and may be considered as the Montgomery representation of another number s'. The trusted third party TTP then computes and stores (step 302) the Montgomery representation of s'^e, i.e., [[ie.]] $s\, x_m\, s\, x_m\, s \ldots x_m\, s$ (e times). The verifier V receives and stores se (step 303) from the trusted third party.